24 hình thức lừa đảo trên không gian mạng

Sự đồng bộ, thay đổi kịp thời của cơ chế chính sách liên quan đến hoạt động thanh toán nói chung và thanh toán thẻ nói riêng; cơ chế phối hợp, chia sẻ thông tin giữa các cơ quan, bao gồm nhưng không giới hạn như Bộ Công an, Ngân hàng Nhà nước, Chi hội Thẻ Hiệp hội Ngân hàng, các tổ chức thẻ và các ngân hàng thương mại được tăng cường; ý thức quản trị rủi ro chủ động của người dùng với các công cụ, phương tiện mà ngân hàng trang bị trong quá trình cung cấp sản phẩm dịch vụ là những điểm mấu chốt để phòng ngừa và hạn chế tối đa tổn thất khi có rủi ro gian lận thẻ xảy ra.

Người dùng các phương tiện thanh toán liên tục nhận được truyền thông từ các ngân hàng, các cơ quan liên quan để có được những thông tin, kiến thức cơ bản để quản trị rủi ro chủ động đối với hoạt động thanh toán của chính mình.

Trong chiến dịch nâng cao nhận thức của cộng đồng, Bộ Công an Việt Nam đã khuyến cáo đến người dân và chính các ngân hàng để phòng tránh cho khách hàng 24 hình thức lừa đảo trên không gian mạng.

1. Lừa đảo "combo du lịch giá rẻ"

* Đăng tải bài viết quảng cáo bán tour du lịch, phòng khách sạn giá rẻ trên mạng Internet và mạng xã hội với nhiều tiện ích kèm theo, đề nghị nạn nhân chuyển tiền đặt cọc (từ 30 - 50% giá trị) để đặt cọc tour du lịch, phòng khách sạn, từ đó chiếm đoạt số tiền đặt cọc.

* Đăng bài viết quảng cáo dịch vụ làm visa (thị thực) du lịch nước ngoài, cam kết tỷ lệ thành công cao, hoàn trả 100% số tiền nếu không xin được visa. Sau khi nạn nhân chuyển khoản thanh toán chi phí hoặc một phần chi phí, các đối tượng sẽ để nạn nhân tự khai thông tin tờ khai, hoàn thiện hồ sơ… Sau đó lấy lý do nạn nhân khai thông tin bị thiếu và không trả lại tiền.

* Các đối tượng giả mạo website và fanpage của công ty du lịch uy tín, làm giả ảnh chụp biên lai, hóa đơn thanh toán và đề nghị nạn nhân chuyển khoản thanh toán chi phí tour du lịch.

* Mạo danh đại lý bán vé máy bay, tự tạo ra các website, trang mạng xã hội, với địa chỉ đường dẫn, thiết kế tương tự kênh của các hãng hoặc đại lý chính thức, sau đó quảng cáo với các mức giá rất hấp dẫn so với mặt bằng chung để thu hút khách hàng. Nếu khách hàng liên hệ, các đối tượng sẽ đặt chỗ vé máy bay, gửi mã đặt chỗ để làm tin và yêu cầu khách hàng thanh toán. Sau khi nhận thanh toán, các đối tượng không xuất vé máy bay và ngắt liên lạc. Do mã đặt chỗ chưa được xuất ra vé máy bay, nên sẽ tự hủy sau một thời gian và khách hàng chỉ biết được việc này khi đến sân bay.

2. Lừa đảo cuộc gọi video Deepfake, Deepvoice

Deepfake là công nghệ ứng dụng trí tuệ nhân tạo (AI) để tạo ra các đoạn video với hình ảnh khuôn mặt nhân vật giống hệt như hình ảnh người dùng muốn giả mạo. Kẻ lừa đảo có thể thực hiện cuộc gọi thoại, thậm chí cả video với giọng nói, hình ảnh là của người thân, người quen, sếp... khiến người nhận rất khó phân biệt thật giả và sập bẫy lừa đảo cuộc gọi Deepfake.

3. Lừa đảo "khóa SIM" vì chưa chuẩn hóa thuê bao

Đóng vai là nhân viên nhà mạng, các đối tượng lừa đảo yêu cầu người dùng cung cấp số chứng minh nhân dân hoặc căn cước công dân để kiểm tra trên hệ thống thuê bao đã đăng ký thông tin chính chủ hay chưa. Nếu người dùng từ chối cung cấp, các đối tượng đưa ra nhiều lời đe dọa sẽ khóa thuê bao di động và "buộc" người dùng làm theo hướng dẫn. Nếu thực hiện theo sẽ có nguy cơ mất quyền kiểm soát SIM điện thoại và kẻ xấu sẽ tiến hành chiếm đoạt các tài khoản khác như mã OTP ngân hàng, tài khoản mạng xã hội...

4. Giả mạo biên lai chuyển tiền thành công

Thủ đoạn của các đối tượng lừa đảo là mua hàng số lượng lớn, sau đó đề nghị chuyển khoản theo hình thức Internet Banking cho người bán hàng. Nhưng thực chất đối tượng không chuyển tiền thật, mà các đã dùng một số phần mềm tạo dựng biên lai (bill) thanh toán giả rồi đưa cho người bán hàng xem nhằm chứng minh là đã thực hiện việc chuyển khoản. Người bán hàng nhìn ảnh bill giả các đối tượng đưa cho, tưởng là thật nên đồng ý giao hàng.

5. Giả danh giáo viên, nhân viên y tế báo người thân đang cấp cứu

Các đối tượng lừa đảo tự xưng là giáo viên, nhân viên y tế, gọi điện cho phụ huynh, học sinh thông báo rằng con em, người thân họ đang cấp cứu trong tình trạng nguy kịch, yêu cầu chuyển tiền đóng viện phí để phẫu thuật gấp, từ đó chiếm đoạt tài sản

6. Chiêu trò lừa đảo tuyển người mẫu nhí

Thủ đoạn của các đối tượng là thông qua mạng xã hội như Facebook, Zalo, Telegram…, các đối tượng lừa đảo sẽ kết bạn với phụ huynh và mời tham gia ứng tuyển người mẫu nhí cho hãng thời trang. Sau khi nạn nhân "cắn câu", các đối tượng lừa đảo sẽ đưa vào một group chat để mời tham gia thử thách. Thử thách cho các phụ huynh khi muốn con mình tham gia vào ứng tuyển "người mẫu nhí" là chuyển khoản để mua sản phẩm hàng hiệu, sau đó cho con em mình làm mẫu chụp ảnh để giới thiệu, quảng bá sản phẩm trên mạng xã hội. Thông thường ban đầu, chúng trả hoa hồng và tiền làm nhiệm vụ để "kích thích" phụ huynh tham gia. Nhưng khi số tiền chuyển vào tài khoản tăng cao, chúng xóa tung tích nhằm chiếm đoạt số tiền đã chuyển.

7. Thủ đoạn giả danh các công ty tài chính, ngân hàng

Các đối tượng lừa đảo tạo lập hàng nghìn tài khoản facebook với các nguồn thông tin giả, tham gia vào các hội nhóm, diễn đàn, đăng bài quảng cáo cho vay tín chấp hấp dẫn...Khi có người vay tiếp cận, các đối tượng sẽ dẫn dụ, yêu cầu người vay cung cấp thông tin cá nhân, như: họ tên, số điện thoại, ảnh chụp CMND/CCCD, ảnh chụp chân dung… phục vụ làm hồ sơ vay.Sau khi dụ người vay chuyển tiền phục vụ hỗ trợ xác minh, duyệt khoản vay, các đối tượng tiếp tục viện dẫn hàng loạt các lý do khoản vay không được giải ngân xuất phát từ lỗi khai hồ sơ của người vay (như khai sai tên người hưởng thụ, đổi cách viết tên người hưởng thụ từ chữ in thường sang in hoa, …). Từ đó, chúng yêu cầu người vay phải nộp thêm các khoản tiền để bảo đảm khoản vay hoặc khắc phục lỗi hệ thống; hứa hẹn sẽ hoàn trả lại số tiền đã gửi cho khách hàng sau khi khoản vay được giải ngân. Tuy nhiên, khi người vay chuyển tiền vào số tài khoản của các đối tượng cung cấp, các đối tượng sẽ lập tức chiếm đoạt và ngắt liên lạc.

8. Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen…

Lợi dụng tính năng cho phép đăng thông tin của trang web như đăng hỏi đáp, diễn đàn, tải tập tin, các đối tượng xấu đưa quảng cáo lên. Các ứng dụng vay tiền trực tuyến hay các link quảng cáo cờ bạc, cá độ thường được quảng cáo rộng rãi trên các trang web với những tiêu đề thu hút như “Không cần thế chấp, lãi suất không đồng”, “Vay siêu tốc, nhận tiền sau 30 phút, lãi suất thấp, nhận tiền ngay”… hoặc nhắn tin qua số điện thoại kèm theo đư ờng link đến ứng dụng…Người có nhu cầu tham gia chỉ cần ấn (click) vào những trang quảng cáo, tải các ứng dụng về máy tính hoặ c điện thoại thông minh, nhập các thông tin cá nhân, số tài khoản ngân hàng nhận tiền, ảnh chứng minh nhân dân, ảnh cá nhân và đồng ý cho truy cập vào danh bạ cá nhân…

9. Giả mạo trang thông tin điện tử, cơ quan, doanh nghiệp (BHXH, ngân hàng…)

Các đối tượng này có thể tạo trang web có giao diện gần giống trang web của cơ quan, doanh nghiệp từ hình ảnh, giao diện và nội dung để người dùng nhầm tưởng là trang web của đơn vị cung cấp. Sau đó, các đối tượng sử dụng tin nhắn giả mạo thương hiệu với các nội dung yêu cầu người dùng phải truy cập vào liên kết giả mạo, khai báo thông tin cá nhân, tài khoản ngân hàng và từ đó thực hiện hành vi đánh cắp, chiếm đoạt thông tin dữ liệu người dùng, lừa đảo. Một số địa chỉ đã từng được các đối tượng sử dụng đều có đường dẫn đến có định dạng bất thường như là vn-cbs.xyz. vn-ms.top…

10. Lừa đảo SMS Brandname, phát tán tin nhắn giả mạo

Các đối tượng sử dụng trạm phát sóng BTS giả mạo để gửi hàng loạt tin nhắn SMS Brandname lừa đảo tới người dùng với mục đích nhằm chiếm đoạt tài sản. Khi làm theo yêu cầu và truy cập vào trang giả mạo, khách hàng sẽ khai thông tin đăng nhập, mật

khẩu, mã OTP, để rồi bị chiếm đoạt quyền quản trị tài khoản ngân hàng ngay tức khắc. Sau đó, đối tượng sẽ thực hiện các giao dịch để chuyển đi toàn bộ số tiền đang có trong tài khoản của khách hàng.

11. Lừa đảo đầu tư chứng khoán, tiền ảo, đa cấp

* Các đối tượng sử dụng thủ đoạn tổ chức hội nghị, hội thảo... lồng ghép giới thiệu quảng cáo về chứng khoán quốc tế, tiền ảo, tiền kỹ thuật số. Mức lợi nhuận vượt trội so với thị trường và dễ dàng rút vốn, lãi là những yếu tố mà các đối tượng đưa ra để lôi kéo người dân, nhà đầu tư.

* Các đối tượng này không cung cấp đầy đủ thông tin về công ty, giấy phép hoạt động, mã số thuế, lịch sử giao dịch, nhân sự quản lý, không được kiểm soát từ cơ quan Nhà nước. Đối tượng yêu cầu người dân, nhà đầu tư chuyển khoản tiền trước khi bắt đầu giao dịch; thường là dưới hình thức phí đăng ký, phí tham gia hoặc tiền ký quỹ. Khi thấy người dân, nhà đầu tư không còn khả năng chuyển tiền, các đối tượng sẽ vô hiệu hóa tài khoản, chặn liên lạc nhằm chiếm đoạt số tiền mà nạn nhân đã chuyển khoản...

12. Lừa đảo tuyển cộng tác viên online

Nắm bắt được tâm lý của nhiều người muốn có công việc nhẹ nhàng, thu nhập cao, các nhóm đối tượng đã sử dụng thủ đoạn lừa đảo thông qua việc tuyển cộng tác viên làm việc online với tỷ lệ hoa hồng lớn - giả mạo các trang sàn thương mại điện tử như Tiki, Shopee, Lazada và các thương hiệu lớn để chiếm đoạt tài sản của các nạn nhân.

Thời gian đầu, với các đơn hàng giá trị nhỏ, nạn nhân sẽ được hưởng hoa hồng đầy đủ. Sau đó, với những đơn hàng có giá trị cao, các đối tượng sẽ chiếm đoạt số tiền các nạn nhân ứng ra để nhận sản phẩm của các đơn hàng. Khoản tiền các đối tượng lừa chiếm đoạt được từ hình thức này thường từ vài triệu đến vài trăm triệu đồng.

13. Đánh cắp tài khoản mạng xã hội, nhắn tin lừa đảo

* Tin nhắn hoặc email đáng ngờ: Nếu bạn nhận được một tin nhắn hoặc email từ một người bạn trong danh sách bạn bè yêu cầu cung cấp thông tin cá nhân nhạy cảm, yêu cầu chuyển tiền hoặc thực hiện hành động khẩn cấp, hãy cảnh giác, vì đó có thể là tin nhắn lừa đảo. Nếu tin nhắn từ bạn bè có dấu hiệu đáng ngờ, cần đề phòng kẻ xấu đã chiếm quyền tài khoản MXH để lừa đảo. Đặc biệt, nếu tin nhắn có chứa các lời khẩn cấp, đe dọa hoặc yêu cầu không phù hợp, hãy kiểm tra lại xem có phải tin nhắn thực sự từ bạn bè của bạn hay không.

* Sự thay đổi đột ngột trong ngôn ngữ hoặc phong cách viết: Nếu tin nhắn từ bạn bè có sự thay đổi đột ngột trong cách viết, từ ngữ không giống với phong cách thông thường hoặc có chứa các lời lẽ lạ lùng, cẩn thận hơn.

* Đường link đáng ngờ: Kiểm tra đường link được chia sẻ trong tin nhắn. Nếu đường link có dấu hiệu đáng ngờ như URL không phổ biến, thiếu ký tự an toàn (https://), hoặc điều hướng đến các trang web không rõ nguồn gốc hoặc đáng ngờ, hãy tránh nhấp chuột hoặc truy cập vào đường link đó.

* Yêu cầu cung cấp thông tin cá nhân hoặc thông tin đăng nhập: Lưu ý rằng bạn không nên cung cấp thông tin cá nhân nhạy cảm hoặc thông tin đăng nhập (tên đăng nhập, mật khẩu) thông qua tin nhắn hoặc email. Kẻ lừa đảo thường sử dụng chiêu này để chiếm quyền điều khiển tài khoản của bạn.

14. Giả danh cơ quan công an, viện kiểm sát, tòa án gọi điện lừa đảo

* Sử dụng số điện thoại giả mạo: Đối tượng sẽ sử dụng số điện thoại giả mạo, có thể hiển thị số điện thoại của cơ quan công an, viện kiểm sát hoặc tòa án trên màn hình điện thoại của bạn. Hãy lưu ý rằng cơ quan chính thức sẽ không sử dụng số điện thoại giả mạo hoặc giả danh.

* Đe dọa và áp lực tâm lý: Đối tượng sẽ sử dụng các cách thức đe dọa, áp lực tâm lý như khống chế, hăm dọa, nói dối về việc có liên quan đến các vụ án đang điều tra để tạo áp lực và đánh vào sợ hãi của nạn nhân.

* Yêu cầu chuyển tiền hoặc thông tin cá nhân: Đối tượng sẽ yêu cầu bạn chuyển tiền vào một tài khoản cụ thể hoặc cung cấp thông tin cá nhân như số thẻ tín dụng, số căn cước công dân, mã số bảo mật và các thông tin nhạy cảm khác. Điều này nhằm mục đích chiếm đoạt tài sản của bạn.

* Tạo áp lực thời gian: Đối tượng thường tạo áp lực thời gian cho bạn, tuyên bố rằng hành động phải được thực hiện ngay lập tức để tránh hậu quả nghiêm trọng. Họ sẽ cố gắng thuyết phục bạn rằng không có thời gian để suy nghĩ hay tham khảo người khác.

15. Rao bán hàng giả, hàng nhái trên sàn thương mại điện tử

* Giá quá rẻ: Sản phẩm được rao bán với giá cực kỳ hấp dẫn, thường rẻ hơn rất nhiều so với giá thị trường. Đây có thể là dấu hiệu của hàng giả, hàng nhái hoặc gian lận.

* Thiếu thông tin sản phẩm: Người bán không cung cấp đủ thông tin chi tiết về sản phẩm, như thông số kỹ thuật, nguồn gốc, chất lượng, thông tin về nhà cung cấp và bảo hành.

* Số lượng giới hạn và áp lực mua hàng: Người bán áp đặt áp lực mua hàng nhanh chóng bằng cách khuyến khích mua hàng ngay lập tức với lý do rằng hàng chỉ có số lượng giới hạn hoặc đang có nguy cơ hết hàng.

* Đánh giá và nhận xét không tự nhiên: Sản phẩm nhận được đánh giá và nhận xét tích cực một cách quá mức, không tự nhiên hoặc không có đáng tin cậy. Đây có thể là một chiêu trò để tạo lòng tin và thuyết phục người mua.

* Phương thức thanh toán không an toàn: người bán yêu cầu thanh toán bằng các phương thức không an toàn, chẳng hạn như chuyển khoản trực tiếp qua ngân hàng, thanh toán bằng ví điện tử không rõ nguồn gốc, hoặc yêu cầu cung cấp thông tin thẻ tín dụng một cách đáng ngờ.

* Tài khoản người bán không đáng tin: Kiểm tra tài khoản của người bán trên mạng xã hội hoặc sàn thương mại điện tử. Nếu tài khoản không đáng tin, với ít hoặc không có thông tin cá nhân, hoạt động mới hoặc không có đánh giá, đó có thể là một dấu hiệu cho thấy người bán không đáng tin cậy.

* Thiếu thông tin liên hệ và địa chỉ: Người bán không cung cấp thông tin liên hệ rõ ràng, như địa chỉ, số điện thoại hoặc email. Điều này khiến việc theo dõi và giải quyết các vấn đề liên quan trở nên khó khăn.

* Thiếu uy tín và phản hồi tiêu cực: Người bán có lịch sử phản hồi tiêu cực, có nhiều khiếu nại từ người mua trước đó hoặc không có đủ đánh giá và phản hồi từ khách hàng.

16. Đánh cắp thông tin CCCD đi vay nợ tín dụng

* Cảnh báo về việc tiết lộ thông tin cá nhân: Sử dụng thông tin trên CCCD để đăng ký mã số thuế ảo hoặc cung cấp thông tin cá nhân như số CMND (chứng minh nhân dân), ngày sinh, địa chỉ trên mạng xã hội có thể rất nguy hiểm. Kẻ gian có thể lợi dụng thông tin này để thực hiện các hoạt động lừa đảo hoặc chiếm đoạt tài sản của bạn.

* Cảnh báo về vay tiền từ các tổ chức tín dụng trên mạng xã hội: Các tổ chức tín dụng trên mạng xã hội có thể cung cấp dịch vụ vay tiền nhanh chóng và dễ dàng. Tuy nhiên, hãy cẩn trọng với các khoản lãi suất cao và các điều khoản vay không rõ ràng. Nếu không thực hiện cẩn thận, bạn có thể rơi vào tình trạng nợ nần và mất tài sản.

* Cảnh báo về lừa đảo chiếm đoạt tài sản: Trên mạng xã hội, có rất nhiều hình thức lừa đảo nhằm chiếm đoạt tài sản của người khác. Họ có thể sử dụng các chiêu thức như làm quen, tạo dựng lòng tin và yêu cầu chuyển khoản tiền hoặc cung cấp thông tin cá nhân. Hãy cẩn trọng với các tin nhắn, cuộc gọi hoặc thông tin từ người không rõ danh tính.

17. Lừa đảo chuyển nhầm tiền vào tài khoản ngân hàng

Các đối tượng cố ý chuyển nhầm tiền vào tài khoản của một người nào đó. Sau khi bên kia nhận được tiền, đối tượng sẽ giả danh là người thu hồi nợ của một công ty tài chính để liên hệ, dọa nạt và yêu cầu họ trả lại số tiền vừa nhận như một khoản vay với số lãi

cắt cổ. Một trường hợp khác, đối tượng lừa đảo chuyển tiền cho người bị hại, sau đó liên hệ giới thiệu mình đang sống tại nước ngoài và muốn được nhận lại số tiền mình chuyển nhầm. Để trả lại số tiền, người nhận tiền phải sử dụng dịch vụ chuyển tiền quốc tế qua một đường link. Sau khi điền đầy đủ thông tin tài khoản ngân hàng vào đường link nói trên, toàn bộ số tiền trong tài khoản của bị hại sẽ bị rút sạch.

18. Lừa đảo dịch vụ lấy lại tiền khi đã bị lừa

Các đối tượng xấu đã đóng vai luật sư, nhân viên ngân hàng, kỹ sư công nghệ thông tin... cung cấp "dịch vụ hỗ trợ lấy lại tiền bị lừa" nhưng thực chất là để đưa nạn nhân "vào tròng" thêm một lần nữa. Các dấu hiệu nhận biết:

* Nghiên cứu mục tiêu, xác định những cá nhân hoặc tổ chức có danh tiếng chân thật và đáng tin cậy.

* Tạo một danh tính giả, hồ sơ giả và các trang hoặc tài liệu giả.

* Thiết lập liên lạc, tiếp cận nạn nhân và những người có liên quan.

* Sử dụng ngôn từ thuyết phục và các chiến thuật để xây dựng lòng tin.

* Yêu cầu thanh toán hoặc cung cấp thông tin cá nhân.

* Tiếp tục giả mạo, cung cấp thông tin cập nhật và sự đảm bảo với nạn nhân.

19. Lừa đảo lấy cắp Telegram OTP

Thường kẻ lừa đảo, tạo một profile giả mạo, đánh cắp hình ảnh của 1 người uy tín có liên quan đến nạn nhân để tạo sự tin cậy: thường dùng sự kiện đáng tin cậy và hấp dẫn để bảo đảm người khác tin tưởng và tham gia vào quá trình.

20. Lừa đảo tung tin giả về cuộc gọi mất tiền như FlashAI

Thông tin rằng chỉ bằng việc nhận cuộc gọi voicecall bạn có thể bị mất tiền như FlashAI hoặc tương tự là KHÔNG chính xác. Không có cách nào để người dùng bị trừ tiền chỉ bằng việc nhận cuộc gọi voicecall thông thường trên điện thoại di động. Việc các đối tượng làm vậy nhằm mục đích câu views, likes và gây hoang mang dư luận xã hội.

21. Lừa đảo dịch vụ lấy lại Facebook

Người dùng mạng xã hội Facebook có thể bị khóa tài khoản trong một số trường hợp như: tài khoản bị hacker chiếm đoạt, bị khóa do chia sẻ nội dung vi phạm tiêu chuẩn cộng đồng của nền tảng...Nhiều kẻ gian lợi dụng tâm lý lo lắng, muốn nhanh chóng lấy lại tài khoản Facebook của người dùng để lừa đảo trục lợi, chiếm đoạt tài sản.

22. Lừa đảo tình cảm, dẫn dụ đầu tư tài chính, gửi bưu kiện, trúng thưởng…

Một số dấu hiệu nhận biết như sau:

* Xác định và tiếp cận nạn nhân: Kẻ lừa đảo tìm và tiếp cận người mục tiêu thông qua các kênh trực tuyến như mạng xã hội, trang web hẹn hò hoặc diễn đàn. Kẻ lừa đảo tạo một hồ sơ giả mạo, sử dụng hình ảnh đánh cắp của người khác với ngoại hình đẹp và lôi cuốn, sau đó sử dụng các chiêu trò lừa đảo để thu hút sự quan tâm của nạn nhân.

* Xây dựng mối quan hệ: Kẻ lừa đảo tạo một mối quan hệ tình cảm giả với nạn nhân bằng cách sử dụng các chiêu trò như tán tỉnh, chia sẻ câu chuyện cảm động hoặc đưa ra lời hứa.

* Dẫn dụ nạn nhân gửi hình ảnh, video nhạy cảm, sau đó dùng những hình ảnh này để đe dọa, tống tiền nạn nhân). Một số kẻ lừa đảo tinh vi thì sử dụng nhiều cách khác nhau để thuyết phục nạn nhân tham gia đầu tư vào thị trường tài chính Forex thông qua một sàn giao dịch giả mạo mà kẻ lừa đảo kiểm soát. (Vì kẻ lừa đảo nắm bắt được tâm lý và tình hình tài chính của nạn nhân).

* Kẻ lừa đảo gửi hàng bưu kiện có giá trị và bắt đóng tiền thuế bằng cách gửi tiền vào tài khoản kẻ lừa đảo. Kẻ lừa đảo có thể đe dọa hoặc lừa đảo nếu nạn nhân không tuân thủ yêu cầu.

* Chiếm đoạt tài sản hoặc tống tiền: Khi tham gia đầu tư tài chính Forex, nạn nhân sẽ bị dẫn dụ thắng vài lần tạo niềm tin và lòng tham, sau đó khi thắng số tiền lớn hơn thì nạn nhân sẽ không rút ra được, bắt phải đóng phí giao dịch, đóng thuế hoặc bảo là tài khoản bị sai thông tin, phải đóng tiền để xác minh chứng thực... Cứ thế cho đến khi nạn nhân hết sạch tiền, phá sản.

23. Rải link phishing lừa đảo, seeding quảng cáo bẩn trên Facebook

Dấu hiệu nhận biết những đường link lừa đảo, quảng cáo "bẩn" trên mạng xã hội:

* Tạo trang web giả mạo: Kẻ lừa đảo tạo một trang web giả mạo có giao diện tương tự như một trang web đáng tin cậy như ngân hàng hoặc dịch vụ trực tuyến. Trang web này được thiết kế để thu thập thông tin cá nhân và đăng nhập của người dùng khi họ nhập vào.

* Tạo một đường link hấp dẫn: Kẻ lừa đảo tạo một đường link hấp dẫn sử dụng một tiêu đề hoặc mô tả mà người dùng có thể quan tâm, chẳng hạn như "Nhận ngay ưu đãi đặc biệt" hoặc "Kiểm tra tài khoản của bạn" hoặc "Bạn bị bóc phốt" hoặc các sự kiện đang hot trending xu hướng trên mạng xã hội. Đảm bảo đường link này giống như một đường link đáng tin cậy để gây thiện cảm và khó phát hiện.

* Rải link và seeding quảng cáo bẩn trên Facebook: Kẻ lừa đảo sử dụng các tài khoản giả mạo hoặc các tài khoản đã bị xâm nhập để rải link và seeding quảng cáo bẩn trên

Facebook. Đăng bài viết, nhận xét, bình luận hoặc quảng cáo với đường link đã được tạo, hấp dẫn người dùng để nhấn vào.

* Lừa đảo và đánh cắp thông tin, tài sản: Khi người dùng nhấn vào đường link lừa đảo, họ sẽ được chuyển hướng đến trang web phishing mà kẻ lừa đảo đã tạo. Từ đó, kẻ lừa đảo có thể thu thập thông tin cá nhân, tài khoản hoặc đăng nhập của họ và sử dụng để lừa đảo hoặc đánh cắp tài sản.

24. Lừa đảo cho số đánh đề

Dấu hiệu nhận biết các thủ đoạn lừa đảo

* Tiếp cận và quảng cáo: Kẻ lừa đảo tiếp cận người khác thông qua các phương tiện như điện thoại, email, tin nhắn hoặc mạng xã hội. Họ quảng cáo về việc cung cấp số lô, số đề may mắn có khả năng trúng thưởng lớn.

* Tạo niềm tin: Kẻ lừa đảo sử dụng các câu chuyện thành công, chứng cứ giả và những lời tán tụng để tạo niềm tin và thuyết phục người khác rằng họ có khả năng đưa ra các số lô, số đề chính xác.

* Yêu cầu đóng phí trước: Kẻ lừa đảo yêu cầu người khác đóng một khoản phí trước để nhận được các số lô, số đề may mắn. Họ thường đưa ra lý do như phí dịch vụ, phí tiên tri hoặc phí đăng ký.

* Đánh số lô, số đề: Sau khi người khác đã đóng phí, kẻ lừa đảo cung cấp các số lô, số đề cho người đó đánh. Họ tạo ra cảm giác rằng những số này sẽ mang lại kết quả trúng thưởng lớn.

* Mất phí nếu không trúng: Trong trường hợp người khác không trúng thưởng, kẻ lừa đảo không trả lại số tiền phí mà người khác đã đóng trước đó. Họ sử dụng lý do rằng đó là một khoản phí không hoàn lại hoặc chi phí liên quan đến việc cung cấp các số lô, số đề.

* Chia hoa hồng nếu trúng: Nếu người khác trúng thưởng, kẻ lừa đảo yêu cầu người đó chia hoa hồng hoặc trả một phần tiền thưởng cho mình dưới danh nghĩa đã cung cấp các số lô, số đề may mắn.